

|  |
| --- |
| Catalogue of Frequently asked questions |
| Client incident management system (CIMS)  June 2020 |

# Contents

[Contents 2](#_Toc46820922)

[Section 1 – Purpose 5](#_Toc46820923)

[Section 2 – What is the client incident management system (CIMS)? 5](#_Toc46820924)

[2.1 What is the CIMS? 5](#_Toc46820925)

[Section 3 – Scope 6](#_Toc46820926)

[3.1 How can I tell if my organisation is in scope for CIMS? 6](#_Toc46820927)

[3.2 CIMS in-scope services 6](#_Toc46820928)

[3.3 Community health services – not in scope for CIMS 8](#_Toc46820929)

[3.4 Consortia 8](#_Toc46820930)

[3.5 Are National Disability Insurance Scheme (NDIS) service providers in scope for reporting incidents in the CIMS? 9](#_Toc46820931)

[Section 4 – Phased implementation 9](#_Toc46820932)

[4.1 Implementation of CIMS for in-scope funded organisations or NDIS providers 9](#_Toc46820933)

[4.2 Implementation of CIMS in department-delivered services 10](#_Toc46820934)

[4.3 Monitoring and oversight teams 10](#_Toc46820935)

[Section 5 – Monitoring and oversight 10](#_Toc46820936)

[5.1 What happens if a service provider submits a paper-based incident report? 10](#_Toc46820937)

[5.2 What happens if an incident report is submitted by a department-delivered service but relates to an alleged incident that occurred during service delivery at an external service provider? 10](#_Toc46820938)

[5.3 What happens if an incident report is submitted by a funded organisation but relates to an alleged incident that occurred in a department-delivered service? 11](#_Toc46820939)

[5.4 If there are multiple organisations providing a service for a client, who is required to submit the report? 11](#_Toc46820940)

[5.5 If the allegation is about a labour hire agency staff member, who is responsible for the reporting and management of the incident? 11](#_Toc46820941)

[5.6 What is the role of Agency Performance and System Support under the monitoring and oversight arrangement? 11](#_Toc46820942)

[5.7 What is the role of child protection under the monitoring and oversight arrangements? 11](#_Toc46820943)

[5.8 What is the role of Disability Client Services under the monitoring and oversight arrangements? 12](#_Toc46820944)

[Section 6 – Management of events not in scope for CIMS 12](#_Toc46820945)

[6.1 What is the process to manage alleged privacy breaches for funded organisations that do not have a direct impact upon a client? 12](#_Toc46820946)

[6.2 How will the department ensure that privacy of information is assured? 12](#_Toc46820947)

[6.3 What about incidents that do not have an impact upon a client but affect staff or carers? 13](#_Toc46820948)

[Section 7 – Parallel processes 13](#_Toc46820949)

[7.1 How will incidents that meet the threshold for reportable conduct be notified to the Commission for Children and Young People? 13](#_Toc46820950)

[7.2 What CIMS information is provided to oversight bodies? 14](#_Toc46820951)

[7.3 Are incident reports used to notify the Commission for Children and Young People about the death of a current or former child protection client? 15](#_Toc46820952)

[7.4 Are section 81 and section 82 referral processes for independent investigation and Suitability Panel still in place? 15](#_Toc46820953)

[Section 8 – The policy 16](#_Toc46820954)

[8.1 How can I find out about the details of the CIMS policy? 16](#_Toc46820955)

[8.2 What are the CIMS policy changes that took effect on 3 February 2020? 16](#_Toc46820956)

[8.3 Does the ‘Client incident management guide’ supersede the ‘Responding to allegations of physical and sexual abuse guidelines’? 16](#_Toc46820957)

[8.4 Does the *‘Client incident management guide’* supersede the *‘Guidelines for responding to quality of care concerns in out-of-home care’*? 16](#_Toc46820958)

[8.5 Does the *‘Client incident management guide’* supersede the *‘Critical client incident management instruction’*? 17](#_Toc46820959)

[8.6 What role does quality of care have in the context of CIMS? 17](#_Toc46820960)

[8.7 What role do Quality of support review guidelines have in the context of CIMS? 17](#_Toc46820961)

[8.8 What is ‘during service delivery’? 17](#_Toc46820962)

[8.9 What if an event involving a client occurs outside of service delivery? 19](#_Toc46820963)

[8.10 When should I report historical disclosures? 19](#_Toc46820964)

[8.11 Incident identification and response 19](#_Toc46820965)

[8.12 Incident reporting 20](#_Toc46820966)

[8.13 Incident investigation 25](#_Toc46820967)

[8.14 Incident reviews 27](#_Toc46820968)

[8.15 CIMS monitoring and oversight 30](#_Toc46820969)

[Section 9 - IT support for service providers 30](#_Toc46820970)

[9.1 CIMS IT overview 30](#_Toc46820971)

[9.2 What is the CIMS webform? 31](#_Toc46820972)

[9.3 What is the CIMS Application Program Interface (API)? 31](#_Toc46820973)

[9.4 How will my organisation learn how to use the CIMS webform and CIR? 31](#_Toc46820974)

[9.5 How do we get access to the department-built CIR? 32](#_Toc46820975)

[9.6 Can the CIMS helpdesk (cims@dhhs.vic.gov.au) provide practice advice? 32](#_Toc46820976)

[9.7 Can the CIMS helpdesk (cims@dhhs.vic.gov.au) provide assistance for organisations using their own IT system/CIMS Application Program Interface (API)? 32](#_Toc46820977)

[9.8 Can the CIMS email address (cims@dhhs.vic.gov.au) assist with eBusiness issues? 32](#_Toc46820978)

[9.9 Why does the system time out when I am working on it? 33](#_Toc46820979)

[9.10 Are there mandatory fields for organisations using their own IT system/ CIMS Application Program Interface (API)? 33](#_Toc46820980)

[9.11 Is ‘Date of last service provision’ a mandatory field? 33](#_Toc46820981)

[9.12 What status descriptions does the CIMS IT use? 33](#_Toc46820982)

[9.13 Should a manager identify a client, staff member or other person in the ‘brief summary of the incident’ field? 33](#_Toc46820983)

[9.14 How do I request an extension of due date for a CIMS investigation or review? 33](#_Toc46820984)

[9.15 What happens if I select ‘restricted access’ on an incident report? 34](#_Toc46820985)

[9.16 What is the difference between the address details that I need to provide in the incident report? 34](#_Toc46820986)

[9.17 When can I resubmit non-major impact incidents if they have been withdrawn by the department? 35](#_Toc46820987)

[9.18 Do I need to save the incident report (department-built client incident register)? 35](#_Toc46820988)

[9.19 Can an organisation submit more documents for an outcome that has already been submitted? 35](#_Toc46820989)

[9.20 How can I tell if my organisation is onboarded to CIMS IT? 35](#_Toc46820990)

[9.21 Can an already approved incident report, follow-up recommendation or outcome be withdrawn? 35](#_Toc46820991)

[9.22 My organisation is not onboarded/registered yet to the CIMS application. How can we report an incident? 36](#_Toc46820992)

[9.23 An organisation is having trouble accessing its client incident register. Can they report outside of the system via the one-off direct submission link? 36](#_Toc46820993)

[9.24 Who is responsible for updating service providers’ user details in the CIMS client incident register? 36](#_Toc46820994)

[Section 10 – Supports for service providers 36](#_Toc46820995)

[10.1 Learning and development 36](#_Toc46820996)

[10.2 Helpdesk service 37](#_Toc46820997)

[10.3 Toolkit 37](#_Toc46820998)

# Section 1 – Purpose

The Department of Health and Human Services (the department) requires all in-scope service providers to report client incidents in the client incident management system (CIMS).

The purpose of this frequently asked questions (FAQs) document is to provide in-scope service providers with a catalogue of commonly asked CIMS questions and responses provided. This includes both policy and information technology queries. Where appropriate, responses have been updated to reflect policy and IT changes that came into effect on 3 February 2020. Further information about these policy changes can be found on the department’s CIMS webpage ([CIMS policy update-1 2020](https://providers.dhhs.vic.gov.au/cims-policy-update-1-2020) and [CIMS Frequently Asked Questions Policy update 1- 2020).](https://providers.dhhs.vic.gov.au/frequently-asked-questions-policy-update-1-2020)

# Section 2 – What is the client incident management system (CIMS)?

## 2.1 What is the CIMS?

CIMS is an end-to-end system for the management of client incidents with a focus on the impact an incident has on a client.

It includes five stages:

**Stage 1: Identification and response**

Identification is when an incident is disclosed to, or observed by, a service provider at any service delivery setting (for example, provider premises, outreach location or a client’s home). This may include disclosure by a client, family member or other professionals, to the service provider.

Response covers the immediate activities undertaken to ensure the safety and wellbeing of clients, staff and visitors, preserve evidence and notify emergency services and family or other support people.

**Stage 2: Reporting**

Reporting captures specific information about the incident. As part of this stage, follow-up is undertaken to ensure the information provided in an incident notification is accurate, and service providers and the department are assured that appropriate actions are being planned and/or undertaken to manage the incident.

**Stage 3: Incident investigation**

An investigation is a formal process of collecting information to ascertain the facts about an incident, which may inform any subsequent criminal, civil, disciplinary or administrative sanctions.

In the context of this policy, the purpose of an incident investigation is to determine whether there has been abuse or poor quality of care of a client by a staff member, carer or another client.

Incident investigations are carried out by service providers (including the department) or external bodies (including the department).

**Stage 4: Incident review**

A review is an analysis of an incident to identify what happened, determine whether an incident was managed appropriately, identify likely causes of the incident, and to apply subsequent learnings to reduce the risk of future harm.

Incident reviews are carried out by service providers (including the department) or external bodies (including the department).

**Stage 5: Analysis and learning**

Analysis and learning includes monitoring and acting on trends identified through the analysis of incident information to enhance the quality of service and supports to clients.

Reporting, investigating, reviewing and analysing incidents helps service providers to review and assess the way in which an incident has been managed, to implement improvements, minimise risk and embed a continuous improvement approach. This supports better client experience and outcomes.

Figure 1: Model for the new CIMS

1. Identification and response
2. Reporting
3. Incident investigation
4. Incident review
(Step 3 or Step 4 is required for major impact incidents.)
5. Analysis and learning.

# Section 3 – Scope

## 3.1 How can I tell if my organisation is in scope for CIMS?

Your organisation is in scope for CIMS if it:

* holds a funding and service agreement(s) with the department and
* is funded to deliver services to clients of the department and
  + is listed as one of the in-scope services in *Client incident management guide*, Appendix C: Scope of this guide.

If you are still unsure, your organisation should check with your key department contact within Agency Performance and System Support.

## 3.2 CIMS in-scope services

### Program: Health services

In-scope services include funded organisations that do not report through the Victorian Health Incident Management System (VHIMS), which includes organisations providing the services types listed below:

* aged care and carer’s support services
* alcohol and drug treatment services
* community palliative care services
* home and community care (HACC) services (for people under 65 and under 50 years for Aboriginal people). Excludes services funded through the National Disability Insurance Scheme (NDIS)
* mental health community support services:
* youth residential rehabilitation
* adult residential rehabilitation
* individualised support packages
* accommodation, respite and community support
* sexual health prevention and community-based care services.

**Program: Department delivered or funded disability services**

Service type:

* department delivered disability accommodation services:
* Group homes
* Ararat Day Program
* disability Justice:
* Disability Forensic Accommodation and Treatment Services (DFATS)
* Disability justice case management
* Specialist Forensic Disability Accommodation (SFDA)
* Forensic Disability State-wide Access Services (FDSAS)
* some NDIS organisations (Only incidents connected to supports and services funded by DHHS are to be reported in CIMS. Effective 1/7/2019, NDIS organisations whose supports and services are funded by the NDIS are no longer required to report incidents in CIMS but must now report incidents to the NDIS Quality and Safeguards Commission. NDIS organisations in receipt of funding from DHHS and the NDIS, are subject to both state-based reporting obligations, depending on the source of the funding for the program connected to the incident).

**Program: Children, youth and families services**

Service type:

* family and community services including:
  + - Aboriginal community-controlled organisations (residential services)
    - early parenting services
    - placement prevention / Families FIRST
    - placement prevention and reunification / Family Coaching Victoria
    - Cradle to Kinder program
    - family intervention services
    - Child FIRST and family services
    - family violence and sexual assault services
* home-based care:
  + pre-permanent care (prior to the finalisation of Permanent Care Order)
  + lead tenant
  + home-based care – general / complex / intensive
  + therapeutic foster care
  + leaving care
* kinship care
* residential care:
  + - residential care – general / complex / intensive
    - therapeutic residential care
* secure welfare services
* statutory child protection services including:
  + - child protection services
    - child protection after hours
* therapeutic care

**Program: Housing and community building services**

Service type:

* department-managed housing including:
  + - public housing (but not community-managed housing – see next section on out-of-scope services)
* homelessness assistance including:
* supported accommodation assistance
* homelessness service support
* transitional housing management
* crisis accommodation services and crisis support services
* long-term housing assistance including:
* long-term assistance
* Public Housing Infrastructure Program.

**Program: Youth services**

Service type:

* refugee minor program
* finding solutions
* youth outreach and diversion services
* adolescent support programs.

Please refer to Appendix C of the *Client incident management guide* for a full list of in-scope and out-of-scope services for CIMS. You can download a copy of the guide from the [CIMS page](http://providers.dhhs.vic.gov.au/cims) on the Service Providers website <http://providers.dhhs.vic.gov.au/cims>.

## 3.3 Community health services – not in scope for CIMS

In April 2017, the Department of Health and Human Services Board agreed to defer the transition of registered and integrated community health services into CIMS). This was to address the potential for overlapping administrative and incident reporting requirements and enable consideration of the most appropriate incident reporting framework for community health services in the future.

This decision applies to the whole of the organisation. It is not specific to particular funded programs. As such all health and human services programs – if delivered by a community health service – are not currently in scope for CIMS.

When this deferral ceases, affected organisations will be advised.

If you have any queries about reporting requirements for community health services, please email [Primary Health Partnerships](mailto:partnerships.primaryhealth@dhhs.vic.gov.au) at <partnerships.primaryhealth@dhhs.vic.gov.au>.

## 3.4 Consortia

In consortia arrangements, all members in the alliance/consortium are listed as parties to the service agreement. Each member organisation agrees to the terms and conditions of the service agreement and is individually bound by them. Each member organisation is responsible to the other members and to the department for the actions of the alliance/consortium and service delivery.

As a consequence, each member of the consortia is required to comply with the requirements of CIMS, including submitting incident information electronically to the department under the organisation name that is party to the service agreement for the consortia.

Consortia members can choose to use their existing IT systems or the department-built client incident register. It does not matter if other consortia members submit client incident information via a different system.

For more information, visit the department’s [Service Agreement](https://fac.dhhs.vic.gov.au/incident-reporting) webpage.

## 3.5 Are National Disability Insurance Scheme (NDIS) service providers in scope for reporting incidents in the CIMS?

NDIS service providers were in scope for the reporting of client incidents in CIMS prior to 1 July 2019.

From 1 July 2019, the NDIS Quality and Safeguards Commission (NDIS Commission) commenced in Victoria. The NDIS Commission implemented the NDIS Quality and Safeguarding Framework which replaces Victoria’s existing quality and safeguard arrangements for NDIS participants and services. NDIS providers must comply with the requirements of the NDIS Commission. This means:

**Victorian NDIS service providers**

From 1 July 2019, registered NDIS providers operating in Victoria will be required to report certain types of incidents to the NDIS Commission, as per the *NDIS (Incident Management and Reportable Incidents) Rules 2018.* Registered NDIS providers are required under Commonwealth law to have appropriate systems in place to respond to any incidents that occur or are alleged to have occurred in connection to the provision of supports or services to NDIS participants.

More information on reportable incidents for NDIS providers is available at: <https://www.ndiscommission.gov.au/providers/reportable-incidents>

**Victorian funded service providers (including in-kind services)**

From 1 July 2019, the Victorian Government requires state-funded providers to continue to comply with existing state-based incident reporting systems (eg: CIMS).

Resource and tools for state-based incident reporting policies are available at:

<https://providers.dhhs.vic.gov.au/cims>

<https://www.education.vic.gov.au/childhood/professionals/needs/Pages/ecisprofessionals.aspx#link99>

**Transitional arrangements**

From 1 July 2019, providers who are in receipt of funding from the Victorian Government and the NDIS will be subject to both state‑based and NDIS Commission reporting obligations.

Queries regarding transitional arrangements can be directed to: [quality&safeguards@dhhs.vic.gov.au](mailto:quality&safeguards@dhhs.vic.gov.au)

# Section 4 – Phased implementation

## 4.1 Implementation of CIMS for in-scope funded organisations or NDIS providers

Reporting client incidents through CIMS applied to department funded organisations and National Disability Insurance Scheme (NDIS)\* providers from 15 January 2018 and for department staff of selected delivered services from 1 October 2018. *(\* Effective 1 July 2019, NDIS organisations whose supports and services are funded by the NDIS are no longer required to report incidents in CIMS but must now report incidents to the NDIS Quality and Safeguards Commission.  Please note however, NDIS organisations in receipt of funding from DHHS and the NDIS, are subject to both state-based - ie: CIMS and NDIS reporting obligations).  Further information about NDIS service provider reporting obligations can be found at :* [*https://www.ndiscommission.gov.au/providers/provider-responsibilities/incident-management-and-reportable-incidents*](https://www.ndiscommission.gov.au/providers/provider-responsibilities/incident-management-and-reportable-incidents)).

The implementation of the CIMS was supported by a suite of resources including a dedicated information webpage, email inbox and helpline phone number for queries, guides and supporting materials of online and classroom-based training programs to support capability-building within the sector.

## 4.2 Implementation of CIMS in department-delivered services

CIMS was implemented across department-delivered services commencing 1 October 2018 and only once a formal change consultation process had been completed.

## 4.3 Monitoring and oversight teams

The establishment of CIMS monitoring and oversight teams within each department division was for quality assurance of client incident information.

# Section 5 – Monitoring and oversight

## 5.1 What happens if a service provider submits a paper-based incident report?

All in-scope funded organisations are required to electronically submit incident information via the CIMS IT solution as of 15 January 2018.

If a service provider submits a paper-based incident report form after this date, the department will contact the reporting organisation and advise of the requirement to resubmit the client incident information via the CIMS.

In-scope funded organisations that have not registered to use the CIMS and are required to report a client incident, must contact the **CIMS helpdesk** ([cims@dhhs.vic.gov.au](mailto:cims@dhhs.vic.gov.au)) immediately for further instruction on how to comply with DHHS reporting requirements .

## 5.2 What happens if an incident report is submitted by a department-delivered service but relates to an alleged incident that occurred during service delivery at an external service provider?

If a client discloses details about an incident that occurred in an external service provider to a department-delivered service (for example, child protection), the department-delivered service is responsible for submitting the incident report in CIMS.

Once the incident report is received by the monitoring and oversight team located within the divisional office, the team will determine whether the incident is alleged to have occurred in the external service provider.

If the alleged incident is deemed to have occurred in an external service provider, the department will contact the relevant chief executive officer of the service provider and delegate management of the incident to the organisation.

The CIMS incident report webform submitted by the department delivered service will be ‘withdrawn’ by the divisional office and returned to them with the rationale: ‘*Incident referred to service provider for appropriate reporting and management*’. No further action is required of the department delivered service after this time.

## 5.3 What happens if an incident report is submitted by a funded organisation but relates to an alleged incident that occurred in a department-delivered service?

If a client discloses an incident that occurred in a department-delivered service to a funded external service provider, the funded organisation must complete the CIMS incident report webform in the CIMS. This ensures that the service provider has met the CIMS reporting requirements.

Once the incident information is received by the department, the department will determine whether the incident is alleged to have occurred in a department-delivered service and advise the relevant area director or child protection director (if appropriate) of the requirement to now manage the incident report as per existing policy requirements.

The CIMS incident report webform submitted by the service provider will be ‘withdrawn’ by the department’s divisional office and returned to the funded organisation with the rationale: ‘*Incident referred to department-delivered service for appropriate reporting and management*’. No further action is required of the service provider after this time.

## 5.4 If there are multiple organisations providing a service for a client, who is required to submit the report?

The service provider that witnesses or first becomes aware of the incident must submit an incident report, whether the service is delivered by a department-delivered service or a funded organisation.

If multiple incident reports relating to the same incident are received, a lead organisation will be identified by the department. The decision to allocate a lead will be dependent upon the details of the incident. For example, if the alleged incident occurred in one service but was disclosed by the client to another service, it would be expected that the lead provider would be the one in which the alleged incident occurred.

## 5.5 If the allegation is about a labour hire agency staff member, who is responsible for the reporting and management of the incident?

The service provider responsible for providing the service at the time of the alleged incident is responsible for the reporting and management of the client incident irrespective of whether the allegation is about a substantive staff member or a labour hire staff member.

In these matters, the service provider is responsible for notifying the labour hire agency that an allegation has been raised about its staff member(s) and, where an investigation or review is required, the expectation for the labour hire agency to lead or participate in any interview with the staff member(s) in question.

## 5.6 What is the role of Agency Performance and System Support under the monitoring and oversight arrangement?

While the review and endorsement of incident information received from in-scope funded organisations is the responsibility of the divisional offices, Local Connections / Health Integration and Partnerships retains responsibility for broader service management and monitoring.

The Agency Performance and System Support teams will continue to review incident reporting data analytics to identify systemic, thematic and operational management issues as part of their broader service management and monitoring oversight role. Incident reports are only one of the inputs to service agreement management and monitoring.

## 5.7 What is the role of child protection under the monitoring and oversight arrangements?

Child protection will retain all existing case planning and placement decisions for child protection clients placed within or managed by a funded organisation.

Once incident information submitted by funded organisations is quality-assured and endorsed, the divisional offices will provide a copy of the report to child protection.

Additional information regarding requirements to inform or consult child protection during the incident management process involving a child or young person in out-of-home care can be found in the *Client incident management guide addendum: Out-of-home care*. Incident reports do not remove the requirement for appropriate case notes to be recorded.

The addendum can be found on the [CIMS webpage](http://providers.dhhs.vic.gov.au/cims) at <http://providers.dhhs.vic.gov.au/cims>.

## 5.8 What is the role of Disability Client Services under the monitoring and oversight arrangements?

Disability Client Services will receive copies of submitted incident reports for clients they case manage. Please refer to *Section 3.2 CIMS in-scope services* of this document for the Disability programs this refers to.

Once incident information submitted by funded organisations is reviewed and endorsed by the divisional office, the divisional office will provide a copy of the report to the relevant Disability Client Services.

# Section 6 – Management of events not in scope for CIMS

## 6.1 What is the process to manage alleged privacy breaches for funded organisations that do not have a direct impact upon a client?

Alleged privacy breaches that do not have an impact upon a client will not be reported through CIMS.

With the commencement of CIMS on 15 January 2018, a new privacy incident report form also became available to allow funded organisations to report privacy incidents. The new privacy incident form is web-based.

The form requires the agency to enter details about the privacy incident, clients involved, immediate risks, and how the incident is being managed and contained. The new form includes fields on information security and practices.

Once the report is submitted, the nominated service provider will receive a confirmation email and a reference number. The report will be received by the department’s divisional privacy officer and directed to the funded organisation’s contract manager within the department (that is, Agency Performance and System Support service plan lead), who will work with the funded organisation on managing the incident as required.

Further information can be obtained from the department’s providers’ webpage at <http://providers.dhhs.vic.gov.au/reporting-incidents>. This landing page has links to report a client incident (CIMS), a privacy breach and a reportable conduct notification.

## 6.2 How will the department ensure that privacy of information is assured?

The department and funded organisations have access to personal information (which includes sensitive information) and health information about clients and staff.

It is critical that the department protects the privacy of this personal and health information.

The department is bound by privacy and other laws, including the:

* *Privacy and Data Protection Act 2014*
* *Health Records Act 2001*
* *Charter of Human Rights and Responsibilities Act 2006*

*Freedom of Information Act 1982.*

Sharing information about clients is a legitimate part of providing services and keeping people safe. However, it is important to note that information may only be shared in accordance with the law. A Privacy Impact Assessment has been conducted on both the *Client incident management guide* and CIMS IT to ensure that CIMS meets all privacy requirements.

The Commissioner for Privacy and Data Protection was also consulted throughout the development of CIMS.

## 6.3 What about incidents that do not have an impact upon a client but affect staff or carers?

CIMS focuses on the impact of an incident on the client, rather than impacts on staff.

This change does not diminish the important and legal responsibilities that service providers and the department have in terms of providing a safe work environment for their employees and responding to workplace health and safety incidents appropriately.

External service providers will need to:

* refer to their own existing workplace health and safety systems and human resources processes to deal with reporting and responding to incidents that impact their staff
  + where an incident impacts both clients and staff, the service provider will need to report and manage the incident according to both systems.

In department-delivered services, the department will need to:

* refer to the Disease/Injury/Near-Miss/Accident (DINMA) approach for incidents that impact department staff
* where an incident impacts both clients and staff, the department will need to report and manage the incident according to both systems.

# Section 7 – Parallel processes

## 7.1 How will incidents that meet the threshold for reportable conduct be notified to the Commission for Children and Young People?

* The Victorian Government introduced a Reportable Conduct Scheme on 1 July 2017.
* Under the scheme, organisations with a high level of responsibility for children are required to notify the Commission for Children and Young People of allegations that any staff member has engaged in ‘reportable conduct’ or ‘misconduct that may involve reportable conduct’.
* The Department of Health and Human Services as well as certain organisations funded by the department are included in the scheme. It is the funded organisation’s responsibility to notify the Commission of potential reportable conduct.
* The [Commission for Children and Young People website](https://ccyp.vic.gov.au/news/reportable-conduct-scheme-forms) provides further information about reporting requirements under the Reportable Conduct Scheme at <https://ccyp.vic.gov.au/news/reportable-conduct-scheme-forms>.
* Further information is available at the department’s providers’ webpage at <http://providers.dhhs.vic.gov.au/reporting-incidents>. This landing page has links to make a reportable conduct notification.

## 7.2 What CIMS information is provided to oversight bodies?

7.2.1 Authorised recipient: Commission for Children and Young People

| **When** | **Rationale for distribution** | **How will reports be provided?** |
| --- | --- | --- |
| All major impact incidents for an out-of-home care client. | Oversight of response to incidents affecting children and young people in out-of-home care. | The Commission has direct access to endorsed or reviewed client incident information via CIMS Qlikview (wiithin 24 hours of it being submitted to the department).  This includes all data submitted for relevant incident reports (including key actions taken by the service provider), follow-up recommendations (investigation, case review or RCA review) and rationale for follow-up action and all investigation and RCA outcomes (including themes and actions). |
| Child protection client subject to the child death inquiry process. | Promote continuous improvement and innovation in policies and practices relating to child protection and the safety and wellbeing of vulnerable children and young persons. | The Commission has direct access to endorsed or reviewed client incident information via CIMS Qlikview. |

#### Commission for Children and Young People

Section 60a of the Commission for Children and Young People Act 2012 provides that 'the Secretary to the Department of Health and Human Services must disclose to the Commission any information about an adverse event relating to a child in out of home care ... if the information is relevant to the Commission's functions.'

The related Memorandum of Understanding between the Secretary and the Commission details the processes supporting this information exchange.

Consistent with the Commission's functions under the Act, the Commission may ask the department for further information, which includes reviews about an adverse event.

The Commission has no legislative basis under s. 60A to request information relating to an adverse event directly from an agency. Where further information, such as more details about actions taken or the outcome of a case review is requested, the department will be required to facilitate provision of the requested information.

7.2.2 Authorised recipient: Office of the Disability Services Commissioner (DSC)

| **When** | **Rationale for distribution** | **How will reports be provided?** |
| --- | --- | --- |
| Incident types within in scope disability service programs (only).  Major impact and non-major impact incidents:  death  Major impact incidents:  injury  poor quality of care  physical abuse  sexual abuse  emotional/psychological abuse  emotional/psychological trauma  financial abuse  inappropriate physical treatment  sexual exploitation – major impact | Independent review and monitoring of the quality of responses provided to clients of disability services.  Monitor improvements to the department’s incident review processes. | The DSC has direct access to endorsed or reviewed client incident information via CIMS Qlikview (within 24 hours of it being submitted to the department).  This includes all data submitted for relevant incident reports (including key actions taken by the service provider), follow-up recommendations (investigation, case review or RCA review) and rationale for follow-up action and all investigation and RCA outcomes (including themes and actions). |

The Commissioners can only see an endorsed major impact incident or reviewed non-major impact incident report (as appropriate) and have the capacity to download information in PDF format.

## 7.3 Are incident reports used to notify the Commission for Children and Young People about the death of a current or former child protection client?

No, incident reports are not the trigger to notify the Commission for Children and Young People about the death of a current or former child protection client. Responsibility for these notifications sits with the Office of Professional Practice (OPP). OPP are advised of the death of a current or former child protection client through a range of mechanisms including via the Coroner or operational directors (as outlined in the Child Protection Manual).

## 7.4 Are section 81 and section 82 referral processes for independent investigation and Suitability Panel still in place?

Yes. Allegations of physical and/or sexual abuse against a registered out-of-home carer involving a child or young person in their care may be required to be reported to the Secretary for independent investigation under s. 81 or s. 82 of the *Children, Youth and Families Act 2005* (the Act). This is in addition to, and concurrent with, requirements under the *Client incident management guide*.

The Act provides for disqualification of an out-of-home care carer where, following an independent investigation, the Suitability Panel determines physical or sexual abuse has occurred and the carer poses an unacceptable risk of harm to children.

A s. 81 or s. 82 report must be made in addition to a client incident report. Further information and the s. 81 or s. 82 report form can be found on the [department’s website](https://providers.dhhs.vic.gov.au) at <https://providers.dhhs.vic.gov.au/>.

# Section 8 – The policy

## 8.1 How can I find out about the details of the CIMS policy?

Three key publications are available on the CIMS webpage for you to gain a better understanding of the CIMS policy and processes:

* *Client incident management guide*
* *Client incident management guide addendum: Out-of-home care*
* *CIMS policy update 1 - 2020*

## 8.2 What are the CIMS policy changes that took effect on 3 February 2020?

The changes (effective from 3 February 2020) to reporting under CIMS include:

* Extending reporting timelines for major impact incidents from 24 hours to three business days of the incident occurring or of the service provider becoming aware of the incident
* Removing the monthly bulk submission of non-major impact incidents so that these incidents are reported within three business days of the incident occurring or of the service provider becoming aware of the incident
* Streamlining the process for major impact incidents, such that incidents that include an allegation of abuse (client-to-client or staff-to-client), poor quality of care, or unexplained injury will proceed automatically to investigation
* Requiring service providers to upload case review outcomes into CIMS IT so the department, as system steward, can be assured that case reviews are occurring in a timely way to improve client outcomes
* Replacing the phrase, ‘alleged perpetrator’ with ‘subject of allegation’.

Please refer to the [CIMS policy update-1 2020](https://providers.dhhs.vic.gov.au/cims-policy-update-1-2020) document on the department’s CIMS webpage for further detail in relation to the policy and IT changes. You may also want to read the [CIMS Frequently Asked Questions document specific to this policy update](https://providers.dhhs.vic.gov.au/frequently-asked-questions-policy-update-1-2020) which is also available on the department’s CIMS webpage.

### 8.2.1 Will the 3 February 2020 CIMS policy changes be applied retrospectively?

Only incidents that occur or the service provider becomes aware of from 3 February 2020 will be subject to the policy changes. Existing incidents within CIMS will be subject to the existing policy and reporting requirements.

## 8.3 Does the ‘Client incident management guide’ supersede the ‘Responding to allegations of physical and sexual abuse guidelines’?

Yes, the Client incident management guide replaces the Responding to allegations of physical and sexual abuse guidelines (RAPSA).

The Client incident management guide provides overarching guidance on the response, reporting, investigation and review of all client incidents, and also provides additional guidance for allegations of physical or sexual assault (Appendix B: Responding to allegations of abuse).

## 8.4 Does the *‘Client incident management guide’* supersede the *‘Guidelines for responding to quality of care concerns in out-of-home care’*?

Yes, the Client incident management guide replaces the Guidelines for responding to quality of care concerns in out-of-home care.

The Client incident management guide provides guidance for incident management of incidents occurring in out-of-home care services, including incident investigations. The Client incident management guide – Out-of-home care addendum provides additional guidance to out-of-home care services providers, including requirements for consulting with child protection throughout the management of a client incident, including where an incident investigation is required.

## 8.5 Does the *‘Client incident management guide’* supersede the *‘Critical client incident management instruction’*?

Yes, the *Client incident management guide’* replaces the *Critical client incident management instruction’.*

## 8.6 What role does quality of care have in the context of CIMS?

The *Client incident management guide* replaces the *Guidelines for responding to quality of care concerns in out-of-home care – technical update 2014*.

The *Client incident management guide* provides guidance about the threshold, and minimum standards, for the investigation of client incidents across all in-scope services. The *Client incident management guide* *Addendum: Out-of-home* care provides specific additional guidance regarding responding to and managing client incidents for children in out-of-home care.

## 8.7 What role do Quality of support review guidelines have in the context of CIMS?

CIMS reviews will replace *Quality of support review guidelines*. The *Client incident management guide* provides guidance about the threshold, and minimum standards, for the investigation and/or review of client incidents across all in-scope services.

## 8.8 What is ‘during service delivery’?

‘During service delivery’ includes:

* when the client is receiving a service (for example, when a staff member is with a client, when the client is on an outing where a staff member is present, or when the client is engaging with a service online or via telephone)
* when the client attends a service provider’s premises, including offices, residential services, respite facilities or day services. This includes the area within the boundaries of the premises, as well as the surrounding area within sight of the premises
* for off-site/outreach services, incidents that occur at the location of service delivery and the surrounding area within sight of that location (for example, when a staff member is providing in-home support or support in the community with the client, even if that support is minimal, such as an hour a month)
* for clients under the care of 24-hour services (for example, residential care, custodial services, supported accommodation or statutory child protection), any incident that occurs.

‘During service delivery’ excludes harm that may occur to a client:

* in the general course of life (for example, when a client is receiving episodic care and an incident occurs when the client is not receiving the services). This exclusion does not apply to clients who are under the care of 24hour services
* where a client is receiving episodic care and an incident occurs when the client is not receiving the services that is unrelated to the services provided
* following adequate and appropriate discharge or release from the department-funded service or following the completion of the service provision period.

An incident that has occurred ‘during service delivery’ is an incident that occurs in any of the following circumstances:

* during provision of an in-scope service
* as a result of, or related to, a deficiency or a potential failure in service provision (for example, through hazards, neglect or inadequacy).

The definition of an ‘incident’ will be met if the event caused harm to a client and occurred ‘during service delivery’.

If an incident occurs during service delivery, it is required to be reported.

### 8.8.1 Additional guidance regarding ‘during service delivery’ in community mental health services

The Mental Health branch has provided the following additional guidance (in addition to CIMS policy requirements). For in-scope community mental health services, ‘during service delivery’ includes:

* telephone calls with clients; for example, when the client is on the phone to a worker and informs the worker they are self-harming as the worker speaks or calls the worker just after an incident of self-harm. The incident would still be happening when the client calls, and the service provider may have to respond by calling an ambulance or suggesting the client goes to hospital for treatment
* face-to-face service delivery and delivering a service in a client's home
* text messages sent by clients to a service; for example, young people texting intermittently to a service reporting what is happening to them at that moment
* an appointment or a conversation with the service
* when clients are on the service premises; for example, if an incident occurs in the waiting room.

For more information about ‘during service delivery’ in community mental health service setting, service providers should speak to their Agency Performance and System Support service plan lead or the Mental Health branch.

### 8.8.2 Additional guidance regarding ‘during service delivery’ in specialist family violence service providers

Family Safety Victoria has provided the following additional guidance (in addition to CIMS policy requirements). In specialist family violence services, ‘during service delivery’ means when a client is receiving a service, such as when:

* staff are working directly with clients either in person or on the telephone
* clients are within the boundaries of the premises or within sight of the premises.

**When should I report historical disclosures?**

Specialist family violence providers should report historical disclosures only when the actual incident occurred during service delivery. For example, historical disclosures relating to past incidents of family violence should not be reported as a client incident. Referrals to child protection or police should still occur in line with the relevant reporting requirements and the Child Safe Standards.

For more information about ‘during service delivery’ in family violence service settings, service providers should also speak to Family Safety Victoria or their Agency Performance and System Support service plan lead.

### 8.8.3 Additional guidance regarding ‘during service delivery’ in alcohol and drug service providers

The Drug Policy and Reform branch has provided the following guidance (in addition to CIMS policy requirements). In community drug and alcohol services, ‘during service delivery’ means when a client is receiving a service, such as when:

* staff are working directly with clients either in person or on the telephone
* clients are within the boundaries of the premises or within sight of the premises.

For more information about ‘during service delivery’ in alcohol and drug service settings, service providers should also speak to the Drug Policy and Reform branch or their Agency Performance and System Support service plan lead.

### 8.8.4 Additional guidance regarding ‘during service delivery’ in lead tenant

Lead tenant is a type of out-of-home care placement and is therefore in scope for CIMS. Like other 24-hour care services (residential care, custodial services and child protection), a client incident report is required for all incidents involving clients of this service, regardless of the location of the incident.

For more information about ‘during service delivery’ in out-of-home service delivery settings, service providers should also speak to the Children and Families Policy branch or their Agency Performance and System Support service plan lead.

### 8.8.5 Additional guidance regarding ‘during service delivery’ in transitional housing management

Transitional housing management is in scope for CIMS, under the banner of the service type ‘homelessness assistance’. The CIMS policy definitions of ‘during service delivery’ applies to transitional housing management services, including consideration of when the client is receiving the service (for example, when a staff member is with a client or when the client is engaging with a service online or via telephone).

Community-managed housing services are out-of-scope for CIMS, meaning that to the extent that the client is a ‘tenant’ of the funded organisation, events occurring within the tenancy are not in-scope for CIMS. Where the service provider is also funded to deliver CIMS in-scope services, such as homelessness assistance services, an incident report for an event occurring during service delivery should be considered.

For more information about ‘during service delivery’ in homelessness assistance services, service providers should speak to the Homelessness and Accommodation Support branch or their Agency Performance and Systems Support service plan lead.

## 8.9 What if an event involving a client occurs outside of service delivery?

During the process of service delivery, different types of events will occur that affect the client. Events that do not meet the definition of a ‘client incident’ are not reported under CIMS.

CIMS does not replace good case management or the requirement to meet other legislative (such as Reportable Conduct Scheme) or policy reporting (such as Privacy policy / reporting breaches) requirements. Service providers are still required to ensure that appropriate communication, client incident records management and other reporting still occurs, even if the event is not a ‘client incident’ under CIMS. See section 3.9 of the Client incident management guide for additional guidance about other reporting.

## 8.10 When should I report historical disclosures?

At times, clients may disclose incidents that occurred in the past. Such incidents should generally be considered in the same way as any other client incident – noting that the appropriate response may be different for an incident that occurred sometime in the past.

For these disclosures, service providers should consider whether the incident occurred during service delivery as defined, including during service delivery by another service provider. If so, the incident should be reported in accordance with the *Client incident management guide* *(Chapter 3.2.2)* unless it has already been reported.

## 8.11 Incident identification and response

**8.11.1 What is new in relation to incident identification and response under CIMS?**

* Clear client-centred minimum standards are identified for responding to all client incidents.
* Specific requirements are identified for preservation of evidence and notification of police, as appropriate.
* Response guidance includes immediate response and planning for ongoing support.
  + Specific guidance for responding to allegations of physical and sexual assault are included.

## 8.12 Incident reporting

### 8.12.1 What is new in relation to incident reporting?

* Revised incident categories and a list of incident types to simplify and streamline classification across services. Service providers select a primary incident type and secondary incident type for each affected client.
* Two categories are used: ‘**major impact**’ and ‘**non-major impact**’. The service provider must exercise professional judgement in identifying the level of impact on each client involved in the incident. All ‘**major impact**’ incidents require specific information to be reported on an individual basis to the department’s divisional office by the service provider, within **3 business days** of the incident occurring or of becoming aware of the incident. *(Note:- Original policy required reporting within 24 hours, however policy change on 3/2/2020 replaced this requirement to reporting ‘within 3 business days’).*
* All ‘**non-major impact**’ incidents will require information (including identifiable details of people involved in the incident) to be reported by the service provider, within 3 business days of the incident occurring or of the service provide becoming aware of the incident. *(Note:- Original policy required a monthly bulk submission process, however policy change on 3/2/2020 replaced this requirement to reporting ‘within 3 business days’)* 
  + Service provider chief executive officers (or senior delegates) are required to review their non-major impact reports and identify patterns of persistent non-major impact incidents for a specific client, which will trigger a major impact incident to reflect cumulative harm, or other patterns of concern.

### 8.12.2 Will the way that service providers report and submit incident reports change?

Yes, the CIMS is online and replaces the former paper-based system of incident reporting.

### 8.12.3 Are there changes to the way incidents are categorised?

Yes, under the CIMS, client incidents are based on the assessment of the impact (level of harm) to the client. The impact of an incident is assessed for each client involved in the incident.

‘**Major impact**’ and ‘**non-major impact**’ define the two incident categories.

**Major impact** incidents include:

* severe physical, emotional or psychological injury or suffering which is likely to cause ongoing trauma
* a pattern of incidents related to one client that, when taken together, meet the level of harm to a client defined above. This may be the case even if each individual incident is a non-major impact incident. This is to reflect the impact of cumulative and persistent harm that is out of the ordinary for the client. This threshold is based on professional judgement and knowledge of the particular circumstances of the client, and the context of the service being delivered
  + the unanticipated death of a client.

Certain incidents have a mandatory requirement to be reported as major impact incidents. For example, all deaths of clients in unexpected or unanticipated circumstances, including suicides and allegations of sexual abuse must be reported as major impact incidents.

For further details, refer to the *Client incident management guide (Appendix A: Definitions of incident types)*.

**Non-major impact** incidents include:

* incidents that cause physical, emotional or psychological injury or suffering, without resulting in major impact as defined above
* impacts to the client that do not require significant changes to care requirements, other than short-term interventions (for example, first aid, observation, talking interventions or short-term medical treatment)
* incidents that involve a client but result in minimal harm
  + incidents that do not otherwise meet the criteria for major impact.

### 8.12.4 How is the impact on clients assessed?

When assessing the effect of an incident on a client, the service provider should use their professional judgement and assessment to consider specific client characteristics that might influence the client’s experience of an incident (for example, the client’s age, development or personal history).

The staff member must exercise their professional judgement to determine what type of incident has occurred.

Factors to consider include:

**Client experience**

* Was the client physically, emotionally or psychologically harmed in the incident? If so, to what extent?
* What level of treatment or care did the client require as a result of the incident?
* Is the client still at risk of further harm?

**Severity of outcome**

* What was the nature and extent of the harm suffered?
* What was the level of distress or suffering caused to the client?

**Vulnerability of client**

* Does the client’s age, stage of development, culture or gender increase the severity of suffering and trauma experienced?
* Does the balance of power or relationship between any alleged perpetrator and victim affect the impact of the incident on the client?
* Does the client’s mental or physical capacity, understanding of potential risks or communication skills affect how the incident impacts them?
* Does the client have a history of trauma or other factors that increase the impact of the incident? For example, abuse, homelessness, social isolation, health status (particularly poor health or other incapacity), poverty and discrimination.

**Pattern and history of behaviour**

* Some clients may have a history of engaging in dangerous activities that are known to the service provider and are being actively case-managed. In cases like this, the service provider may classify an incident as a non‑major impact incident, because it is not unusual for that particular client – even though it might be considered otherwise with another client or in another circumstance.
* However, if the event is linked to either of the following, it should be reported as a major impact incident:
  + - an **escalation** in the severity or frequency of dangerous actions (for example, a client who has been known to get into physical altercations from time to time has recently been doing so on a daily basis)
    - **abnormal** actions outside the known behavioural patterns of that client.

### 8.12.5 How do we determine impact for absent clients?

The CIMS incident type ‘absent client’ requires the service provider to exercise their professional judgement to assess the **concerns for the safety** of the absent client.

* For children and young people in particular, factors for service providers to consider in their assessment impact include:
  + - if there is an escalation in the frequency of the young person’s behaviour, or the behaviours are inconsistent with the young person’s usual behaviour, the event should be assessed as a major impact incident
    - if the young person is absent for short periods of time, is actively engaged with the service provider throughout the absence and the care team is monitoring the absence, the event could be assessed as a non-major impact incident
    - has a warrant been issued?
    - have police been notified?
    - is there a history of sexual exploitation?
    - is this client missing a curfew significant? That is, is the curfew court ordered?
    - is the client a known, high-risk client?
* For all clients:
  + - what is the vulnerability of the client?
    - what is the client’s age?
    - does the client have a history of high-risk behaviours?
    - do the client’s actions require a change of intervention/support for the client?
    - have the actions taken by the client placed them in imminent risk of harm?
    - does the incident categorisation reflect cumulative harm, or patterns of concern?

Does the incident report:

* explain the safety concerns for the client?
* describe the severity of concerns and how that relates to the assessment of risk/impact?
* describe the actions that have been taken to locate the client?
* describe the actions that have been taken to modify the case management, care arrangements or other support supports of the client as a result of the incident?

### 8.12.6 How do we determine impact for dangerous actions taken by the client?

The CIMS incident type ‘dangerous actions - client’ requires the service provider to exercise their professional judgement to assess client actions that **cause the client harm or place the client at risk of harm**.

This includes:

* dangerous actions as a result of the misuse of drugs, alcohol or other substances
* high-risk activities such as arson or train surfing
* sexually orientated actions by a client in circumstances that place their safety at risk.

For children and young people in particular, factors for service providers to consider in their assessment of incident impact include:

* if there is an escalation in the frequency of the young person’s behaviour or the behaviours are inconsistent with the young person’s usual behaviour, the event should be assessed as a major impact incident
* have police been notified?
* is the client a known, high-risk client?

For all clients:

* what is the vulnerability of the client?
* what is the client’s age?
* does the client have a history of high-risk behaviours?
* do the client’s actions require a change of intervention/support for the client?
* have the actions taken by the client placed them in imminent risk of harm?
* does the incident categorisation reflect cumulative harm, or patterns of concern?

Does the incident report:

* explain the safety concerns for the client?
* describe the severity of concerns and how that relates to the assessment of risk/impact?
* describe the actions that have been taken to modify the case management, care arrangements or supports for the client as a result of the incident?

### 8.12.7 How do we determine impact for medication errors?

The CIMS incident type ‘medication error’ requires the service provider to exercise their professional judgement to assess the impact of any error in the administration of a client’s prescribed medication, where the service provider is responsible for such administration. Including:

* the administration of incorrect medication
* missed medication
* the incorrect or unauthorised administration of PRN restraint medication
* psychotropic medicines misuse
* client refusal of prescribed or authorised medication pharmacy error (an error in the dispensing of medication).

This requires the service provide to understand the nature and purpose of medication that they are responsible for administering to clients and the risk of harm to clients as a consequence of any medication error, including missed medication.

Misuse of psychotropic medicines administered by a staff member must be reported as major impact. This includes where administration of this medication is ‘missed’.

### 8.12.8 If a client is absent (as defined under CIMS) and as a result of their absence has missed prescribed medication that the service provider is responsible for administering, does this need to be reported?

Yes, the service provider is required to assess the impact of the missed medication in this situation. Subject to the service provider’s assessment, the primary incident type in this case is likely to be assessed as ‘absent client’. In addition, the service provider could consider reporting the missed medication as a secondary incident type of ‘medication error’ because the client’s absence has prevented the required administration of a prescribed medication.

### 8.12.9 Are there changes to incident types?

Yes, there are changes to incidents types under CIMS. For definitions of incident types, see *Client incident management guide* (*Appendix A: Definitions of incident types)*.

Incident type is assessed for each client impacted by the incident. It is possible to assess both a primary and secondary incident type for each client involved in the incident.

### 8.12.10 Is it possible to map the CIMS incident types to compare them against the previous incident types?

No, it is not possible to directly map the CIMS client incident types to previous client incident types. The CIMS approach to categorising client incidents (major and non-major impact on the client) does not directly correlate with previous reporting mechanisms.

### 8.12.11 Will any type of incidents from the previous incident reporting system no longer be reported?

Events that impact staff or potential privacy breaches will not be reported in CIMS unless there is a client impact associated with these events.

However, it remains important to report these events and they should be reported in workplace health and safety and privacy reporting systems, respectively.8.18.3 If an incident has two incident types, which one should be reported as the primary incident type vs the secondary incident type?

The most serious of the reported incident types, with the greatest impact on the client, should be reported as the primary incident type, and will drive the response to, and management of, the incident by the service provider.

### 8.12.12 When do service providers consult with child protection regarding a client incident in out-of-home care?

Service providers must consult with child protection during the incident management process as detailed within the *Client incident management guide addendum: Out-of-home care* if the client is a child involved with child protection.

The service provider must inform the child protection area manager:

* when a client incident is identified
* when the incident is assessed as having a major impact incident and the report alleges abuse, poor quality of care or unexplained injury, as part of the process to determine the way forward
* of the progress of any investigation involving a child in the care of the department
* of the intention to interview a child or young person as part of an incident review (case review or root cause analysis).

The child protection area manager will consider the impact on the client and the immediate safety of the child, including any decisions regarding the appropriateness of the placement.

In addition, the service provider and child protection would be expected to discuss any client incident as a standard part of good case management practice, including case planning and care team discussions.

### 8.12.13 How will the CIMS ensure impact is assessed appropriately?

The overarching aim of the CIMS is to support the safety and wellbeing of clients and is premised on service providers’ assessment and professional judgement.

Support will be provided to build the capability of service provider staff, including understanding how to appropriately categorise the impact of an incident on a client. This support will include:

* learning and development modules
* the CIMS toolkit
  + the CIMS helpline, which will provide guidance and information to service providers.

In addition:

* Every major impact incident report will be reviewed and endorsed by the department’s divisional office.
* Every non-major impact incident will be quality-assured by the department’s divisional office.
* If issues are identified, feedback will be provided directly to the service provider and the service provider will be asked to resubmit the incident report.

### 8.12.14 Are there changes to reporting timeframes?

Yes, there are changes to the timeframes that apply when client incident information is submitted to the department:

* a major impact incident report must be submitted to the department’s divisional office within three business days of the service provider becoming aware of the incident. (*Please note, this requirement came into effect on 3/2/2020. Prior to this date, the reporting timeline of major impact incidents was within 24 hours.)*
* non-major impact incidents must be recorded on the service provider’s client incident register (CIR) and submitted to the department’s divisional office three business days. *(Please note, this requirement came into effect on 3/2/2020. Prior to this date, the reporting timeline of non-major incidents was that the service provider submit these incidents in bulk on a monthly basis)*

### 8.12.15 How will the department’s divisional office respond to service providers’ new reporting timeframes?

| **Service provider responsibility** | **Department’s divisional office response** |
| --- | --- |
| A major impact incident report must be submitted to the department’s divisional office **within 3 business days** of the service provider becoming aware of the incident. | Endorse the major impact incident report within one business day of submission. |
| Non-major impact incidents must be recorded on the service provider’s client incident register (CIR) and submitted to the department within **3 business days** of the service provider becoming aware of the incident. | Conduct quality assurance of non-major impact incidents submitted within 14 business days of receipt. |
| For major impact incidents, if a full investigation is required, the service provider must submit an investigation outcome report within **28 business days** of incident report endorsement | Endorse the service provider’s investigation outcome report within 14 business days of receipt. |
| Investigation outcome and root cause analysis reports must be finalised and submitted within **60 business days** of incident report endorsement. | Endorse the service provider’s root cause analysis review outcome report within 14 business days of receipt. |
| Investigation outcome and case review reports must be finalised and submitted within **28 business days** of incident report endorsement. | Conduct quality assurance of service provider case reviews via the CIMS performance audit. |

### 8.12.16 Are client incident reports de-identified in the CIMS?

No, the CIMS identifies clients and staff involved in all incidents.

The department has conducted privacy impact assessment on the CIMS policy and CIMS IT. The Commissioner for Privacy and Data Protection was consulted throughout the development of the CIMS.

## 8.13 Incident investigation

### 8.13.1 What is new in relation to investigations?

* All allegations of abuse (sexual, physical, psychological or financial abuse), poor quality of care or unexplained injury must be investigated. *(Please note, this requirement came into effect on 3/2/20. Prior to this date, such incidents were ‘screened’ for investigation).* Investigations are the responsibility of the service provider (including the department where it is the service provider).
* The *Client incident management guide* includes minimum standards for an investigation, clear thresholds for when an investigation is required, and guidelines for when an external investigator should be commissioned and oversight/quality assurance. The service provider is required to have robust, documented processes for investigations and is required to submit the investigation report to the department’s divisional office for quality assurance.
* In exceptional cases, including where the service provider has demonstrated a lack of capacity to conduct an investigation that meets the standards in the *Client incident management guide*, the department may become involved in the investigation as joint investigation manager or investigation manager.
* Investigation outcomes will be electronically submitted to the divisional office for quality assurance via the service provider’s client incident register.
* Employment and carer schemes and screening processes such as the Suitability Panel and Disability Worker Exclusion Scheme will continue.
* The *Guidelines for responding to quality of care concerns in out-of-home care – technical update 2014* is superseded by the new the CIMS.

### 8.13.2 Are all service providers expected to conduct CIMS investigations?

Yes, service providers are required to lead CIMS investigations. Service providers are supported to develop capability to conduct investigations through:

* the *Client incident management guide*, which outlines the threshold and minimum standards for investigations;
* Online learning modules to enhance service providers’ capability to conduct investigations. *(Please note, when CIMS was first implemented, classroom-based training was also provided. This resource is currently no longer available).* 
  + the CIMS toolkit, which includes resources and templates to assist service providers in conducting investigations.

In exceptional cases, including where the service provider has demonstrated a lack of capacity to conduct an investigation that meets the standards set out, the department may become involved in the investigation as joint investigation manager or investigation manager.

### 8.13.3 When is an external investigation required?

Service providers must consider how the independence requirements of an investigation can be met in a given case. Depending on the nature of the incident and the organisation, one of the following may be appropriate to conduct an investigation:

* an area of the organisation that is sufficiently independent from staff who are the subject of any allegations, such as another division or an independent investigative function
* another service provider independent from the staff who are the subject of any allegations
  + an external investigative body.

In exceptional cases, including where the service provider has demonstrated a lack of capacity to conduct an investigation that meets the standards set out, the department may become involved in the investigation as joint investigation manager or investigation manager.

### 8.13.4 What are the investigation timeframes?

Key timeframes for investigations under CIMS are:

* if a **full investigation** is to be undertaken, the investigation report must be finalised and submitted **within 28 business days** of incident report endorsement.
* **Investigation outcome and case review reports** must be finalised and submitted **within 28 business days** of incident report endorsement.
* **Investigation outcome and root cause analysis reports** must be finalised and submitted **within 60 business days** of incident report endorsement.

Timeframes exclude any time that the investigation is put on hold as directed by Victoria Police.

## 8.14 Incident reviews

### 8.14.1 What is new in relation to incident reviews?

* In the context of the CIMS, an incident review is defined as ‘*an analysis of an incident to identify what happened, determine whether an incident was managed appropriately, and to identify the causes of the incident and subsequent learnings to apply to reduce the risk of further harm’ (Chapter 5.1.1 Definition of an incident review* in the *Client incident management guide).*
* There are two types of incident reviews:
  + - Case review – a review led by the service provider following a client incident to identify what happened and any process and system issues. This is a less structured and resource-intensive review than a root cause analysis review. Must be completed within 21 business days.
    - Root cause analysis (RCA) review – a structured review process for identifying the basic or causal factor(s) that underlie an incident, in order to facilitate learning from that incident. It requires trained staff and appropriate resourcing and time, and therefore is only required in certain defined cases. Must be completed within 60 business days.
* The purpose of a review is to determine whether the management of an incident was handled appropriately and to identify any learnings to apply in future.
* In exceptional circumstances where there is a demonstrated lack of capacity of the service provider to undertake an RCA review, the department will have an option to jointly manage the review, with the right to approve the terms of reference and select an independent reviewer.
* Where there are concerns about a service provider’s performance more generally, beyond an individual incident, funded organisation performance monitoring mechanisms such as service reviews would be activated. These are to be distinguished from incident reviews.
* It is noted that external oversight bodies also conduct reviews, and that some of these reviews occur pursuant to legislative processes. These types of reviews will continue in accordance with current approaches.
* The *Quality of support review guidelines* are superseded by the CIMS.
* More information about reviewing incidents can be found in *Chapter 5* of the *Client incident management guide.*

### 8.14.2 Are all service providers expected to lead CIMS reviews?

Yes, service providers are required to conduct CIMS reviews, both case reviews and root cause analysis reviews.

In exceptional circumstances where there is a demonstrated lack of capacity of the service provider to undertake a root cause analysis review, the department will have an option to jointly manage the review, with the right to approve the terms of reference and select an independent reviewer.

### 8.14.3 What outcomes get substantiated as a result of a CIMS investigation?

The purpose of an incident investigation by a service provider under CIMS is to determine whether there has been abuse or neglect of a client by a staff member (including a volunteer) or another client, as a result of an allegation in a client incident report.

The service provider must conduct an investigation if it is a major impact incident within the following categories:

* physical abuse
* sexual abuse
* financial abuse
* emotional/psychological abuse
* poor quality of care
* injury – unexplained (in order to determine whether there has been any abuse or neglect that caused the injury).

The service provider must determine which one of the following investigation options is appropriate:

* Internal investigation
* External investigation
* No further investigative action – in a small number of cases, the service provider may make the decision to take no further investigative action. This may be appropriate where it can be clearly established that the report of the incident is inaccurate or there is no basis for concerns about the safety of the client or the quality of care the client is receiving. If the decision is not to undertake an investigation, the grounds for this decision must be supported and recorded with a persuasive rationale backed up by evidence. **The major impact incident must then be the subject of a review (case review or root cause analysis review)**.

At the conclusion of an investigation either abuse or neglect are substantiated under the following categories:

* physical abuse (as a result of an allegation of physical abuse or incident type unexplained injury)
* sexual abuse
* emotional/psychological abuse
* neglect (as a result of an allegation of poor quality of care or incident type unexplained injury)
* financial abuse

Or, if the above outcomes cannot be substantiated, the outcome of the investigation report will be either:

* not substantiated – no further action – where there is no evidence that the alleged incident took place
* not substantiated – further action – where there is insufficient evidence to substantiate abuse but there is a need for further actions to be taken to address any ongoing concerns.

Some additional considerations for service providers finalising an investigation outcome report include:

* incident types are not ‘substantiated/not substantiated’ – abuse or neglect are ‘substantiated/not substantiated’
  + for example, the result of an investigation into an allegation of ‘poor quality of care’ is that neglect is substantiated/not substantiated; the result of an investigation into a major impact incident under ‘unexplained injury’ is that abuse or neglect is substantiated/not substantiated.
* if the incident report is subject to two incident types that meet the threshold for investigation, then outcomes for both allegations must be documented
  + for example, where there is an allegation of both physical abuse and poor quality of care.
* outcomes should be reported at a client level not report level
  + for example, where two clients are the alleged victims of the same incident, outcomes must be reported for both clients.
* for the purposes of a CIMS investigation abuse or neglect can only be substantiated where the subject of allegation is a staff member or another client (abuse only)
  + for example, it cannot be a member of the public. In these circumstances, for major impact incidents, a case review or root cause analysis review is required, not a CIMS investigation.
* an investigation is likely to uncover issues not identified at the point of incident report
  + if the matters discovered are an extension of the incident reported, then they should be dealt with in the same investigation process and outcome report
  + if the matters discovered relate to a separate/different incident, then an additional incident report should be initiated by the service provider and managed accordingly
  + for example, throughout the course of an investigation into physical abuse, the service provider discovers an allegation of poor quality of care related to the same incident, this should be included in the scope of the investigation and both abuse and neglect substantiated / not substantiated. The investigation and outcome report and action plan should reflect this, and the outcome reporting via the CIMS IT should reflect this also (it is possible to report up to two outcomes in the CIMS application).
  + the investigation process may also deliver findings outside the scope of the CIMS investigation. These findings can be documented within the investigation outcome report, subject to appropriate consideration of privacy and due process issues.

### 8.14.4 Does the department receive the case review outcome report?

When the CIMS was first implemented, service providers were not required to submit case review reports to the department. However, a number of policy changes were made on 3 February 2020, which now includes the requirement that upon completion of the case review, service providers must now submit the case review outcome report, themes (if applicable) and relevant supporting documentation to the department.

Chapter 5 in the *Client incident management guide* provides guidance in relation to the information required. Case review templates, while not mandated, have been developed by the department to assist service providers in identifying relevant information.

Service providers are required to complete case reviews within 21 business days.

### 8.14.5 Finalising a case review outcome report

When the case review is completed, the following steps are required:

* The service provider’s chief executive officer or senior delegate must carefully consider the report and determine whether it meets CIMS requirements.
* The service provider’s chief executive officer or senior delegate approves the case review and ensures that any changes relevant to the services provided to the client are recorded in the client’s file.
* To support the department in efficiently discharging its system steward role, service providers are required to submit the outcomes of all case reviews to the divisional office. The divisional office will retain a copy of the case review report on the CIMS IT. This will enable the department to attest that case reviews are being completed in a timely manner, and to the expected standard. However, case review documents and outcomes will not be subject to a dedicated quality assurance process and will not require endorsement by the department.
* The service provider must log any determined actions against the incident and record when they have been carried out. Actions relevant to the client’s ongoing service provision should also be recorded on the client’s file.
* Service providers must communicate the findings of reviews to the people involved in the incident (including the client and their guardian, family member, key support person or case manager/planner).

### 8.14.6 Can my organisation use its own investigation/review template?

Yes, service providers are able to use their own investigation templates.

While the use of CIMS templates is not mandatory, there is a need to ensure that all information requirements as specified on the department’s template are being captured and provided.

Service providers are recommended to use the CIMS templates available on the department’s [CIMS webpage](https://providers.dhhs.vic.gov.au/cims).

### 8.14.7 Can the authority of the service provider’s chief executive officer be delegated?

Ultimately, the service provider’s chief executive officer is accountable for all incident submissions to the department and oversight of incident management within their organisation. However, the chief executive officer can nominate other senior delegates to act on their behalf.

Authorisation responsibility needs to be maintained at an appropriately senior level.

If the department’s divisional office returns (withdraws) an incident report for rework by the service provider, the service provider’s chief executive officer or the delegated authority who approved the incident information for submission is advised.

## 8.15 CIMS monitoring and oversight

### 8.15.1 Why is my incident/follow-up/outcome being ‘withdrawn’ by the department?

The department has a role in the review, quality assurance and endorsement of incident information. This role is performed by the department’s divisional office (monitoring and oversight team).

In reviewing submitted incident information, the divisional office will assess whether the information meets CIMS policy requirements. If it is assessed that the submitted incident information does not meet the policy requirements, it will be returned to the service provider for immediate rework and resubmission.

In some instances, incident reports are withdrawn because they are out of scope for CIMS (that is, they relate to an event that does not meet the definition of a client incident). In these cases, service providers are not required to resubmit these reports. The information provided by the divisional team about the reason for withdrawal will identify such cases.

If a service provider has any questions about why an incident has been withdrawn by the divisional team, it should contact the team that reviewed that incident via email:

* East Division: EastCIMS@dhhs.vic.gov.au
* West Division: CIMS.West@dhhs.vic.gov.au
* North Division: CIMS.North@dhhs.vic.gov.au
* South Division: South.CIMs@dhhs.vic.gov.au

### 8.15.2 How quickly should I resubmit an incident after it has been withdrawn by the department?

Each stage of the CIMS incident management process has submission timelines that the service provider must comply with. If an incident is withdrawn by the divisional office because the information submitted does not meet the required standards of the CIMS policy, these timelines still apply. It is critical that the service provider assesses withdrawn incidents, makes required changes and resubmits them **immediately**.

In the case of withdrawn non-major impact incidents, service providers should not wait to resubmit a non-major impact incident; it should be reviewed, revised and resubmitted **immediately**.

# Section 9 - IT support for service providers

## 9.1 CIMS IT overview

To support capacity for greater consistency and improved analytics regarding client incident management, the CIMS IT solution was developed.

The IT solution for CIMS includes:

* Client incident register (CIR) and CIMS incident report webform
  + - All service providers are required to have their own CIR to be able to store and transmit client incident reports, investigations and reviews.
    - The department has built a CIR for department-delivered services including child protection, disability accommodation services and secure welfare.
    - Funded organisations may use the department-built CIR.
    - For service providers that use the department-built CIR, the CIMS incident report webform allows service provider staff to report a client incident. A CIMS incident report must be approved by the organisation’s chief executive officer or senior delegate before being submitted to the department’s divisional office for endorsement.
* Application Program Interface (API)
  + - The CIMS API allows external service provider systems to electronically submit client incident information from existing IT platforms to the department.
* Reporting and analytics module
* The system used by the department to monitor, report and analyse incident information submitted by service providers.

## 9.2 What is the CIMS webform?

* The CIMS webform will be accessible to anyone who has access to the internet.
* Staff do not require access to the secure CIR to access and complete the CIMS webform.
* Service provider staff will complete the CIMS webform to report a client incident and submit it within their organisation for quality assurance and approval (which is actioned within the CIR).
* The CIMS incident report must be approved by the service chief executive officer or senior delegate before being submitted to the department’s divisional office to endorse.

## 9.3 What is the CIMS Application Program Interface (API)?

An API is essentially an electronic doorway that allows information to pass through as long as it meets the following criteria:

* It is coming from an authorised source (a registered organisation).
* The information being passed through meets a set criterion.
* For example, ‘DHHS Area’ has 21 set value options that are allowed to pass through the CIMS API doorway. If the value provided by the service provider does not equal one of these 21 values, then it will not be allowed to pass through.

For every field within CIMS IT that has a predetermined value and format, these values and formats are found within the CIMS API reference data that can be accessed by IT vendors to check to make sure that they are using the correct information.

When an attempt to submit an incident/follow-up recommendation/outcome fails, the CIMS API provides a validation failure message to advise the user. These error messages will also provide a reason why the submission was not accepted.

## 9.4 How will my organisation learn how to use the CIMS webform and CIR?

Users can learn how to use the CIMS webform and CIR via the:

* CIMS IT online learning modules
* Training environment incident report webform
* CIMS IT user guides

The weblink for the department’s CIMS learning and development materials/resources is CIMS <https://providers.dhhs.vic.gov.au/cims-learning-and-development>

## 9.5 How do we get access to the department-built CIR?

Service providers are required to ensure that they are registered to use CIMS it to submit and manage incident information.

If a service provider is not fully registered to use the CIMS application and need to report a major impact incident as required under the CIMS policy, the service provider’s chief executive officer or senior delegate should contact the CIMS helpdesk via email <CIMS@dhhs.vic.gov.au>. The CIMS helpdesk will arrange a one-off link that will enable the service provider to submit one major impact incident. After that, the service provider is required to complete the CIMS IT registration and onboarding process immediately.

## 9.6 Can the CIMS helpdesk (cims@dhhs.vic.gov.au) provide practice advice?

No, the CIMS helpdesk cannot provide practice advice or a ‘secondary consultation’ because the helpdesk is not made up of practitioner experts.

The role of the CIMS helpdesk is to assist service providers by providing guidance and support in relation to CIMS policy, resources and the department built CIMS IT.

CIMS is premised on the service provider’s professional judgement and assessment in relation to the client and service delivery environment.

If service provider staff need practice advice, they should in the first instance refer to their own management, their key department contact (Agency Performance and System Support service plan lead) or the relevant department program area.

For incidents involving child protection clients, the *Client incident management guide addendum: Out-of-home care* identifies where it is mandatory for the service provider to inform or consult with child protection throughout the management of a client incident.

## 9.7 Can the CIMS helpdesk (cims@dhhs.vic.gov.au) provide assistance for organisations using their own IT system/CIMS Application Program Interface (API)?

No, the CIMS helpdesk is unable to assist with IT problems for organisations using their own IT system/CIMS API.

This is because every one of those systems is different and may use different terminology, formats and functionality to the department built CIMS IT. Service providers are asked to refer to their organisation’s internal IT processes for these queries (for example, contacting your IT vendor).

IT vendors can report CIMS API problems to the [CIMS Technical Support team](mailto:CIMS.API@dhhs.vic.gov.au) for investigation via <CIMS.API@dhhs.vic.gov.au>. The CIMS Technical Support team will work with the IT vendor and advise them of the resolution of issues. It is the responsibility of the IT vendor to advise their service provider clients (users of their IT system) of the resolution of these issues.

## 9.8 Can the CIMS email address (cims@dhhs.vic.gov.au) assist with eBusiness issues?

eBusiness is a platform used by the department that enables service providers to access a range of department applications, including CIMS IT.

If the service provider has been fully onboarded to the CIMS and a staff member needs to be registered to use eBusiness, is having trouble logging into eBusiness or has a problem with their eBusiness log-in, that staff member should obtain the appropriate [eBusiness](https://hns.dhs.vic.gov.au/dhsportal/wps/myportal) help via one of the following contact methods:

* Phone – 1300 799 470
* Email – ebiz@dhhs.vic.gov.au
* Online eBusiness registration - <https://hns.dhs.vic.gov.au/dhsportal/wps/myportal>.

## 9.9 Why does the system time out when I am working on it?

There is no ‘time-out’ function built into the CIMS application. The time-out experienced by CIMS IT users is due to the eBusiness platform which has a pre-set timeout of three minutes and applies to all department applications accessed via eBusiness.

Users are advised to regularly move their computer mouse, to reduce the risk of the system timing out.

## 9.10 Are there mandatory fields for organisations using their own IT system/ CIMS Application Program Interface (API)?

Yes, organisations using their own IT system / CIMS API have the same mandatory field requirements as service providers using the department-built client incident register.

However, the field names used and how screens are presented and flow vary among these systems. In addition, sometimes organisations using their own IT system / CIMS API capture more than CIMS-related information only, for example, occupational health and safety and organisational risk information.

Department staff, including the CIMS helpdesk and CIMS Technical Support cannot see these systems or how information is presented or organised. When a service provider is using their own IT system / CIMS API and are experiencing problems in the submission of client incident information, they must consult with their manager / own organisation’s IT helpdesk and/or their API vendor to resolve issues.

## 9.11 Is ‘Date of last service provision’ a mandatory field?

No, ‘Date of last service provision’ is not a mandatory field.

## 9.12 What status descriptions does the CIMS IT use?

See Appendix C of the [*Client incident register user manual*](https://providers.dhhs.vic.gov.au/sites/default/files/2020-02/Client%20incident%20register%20user%20manual%20-%20Client%20incident%20management%20system.docx)for CIMS IT status descriptions.

## 9.13 Should a manager identify a client, staff member or other person in the ‘brief summary of the incident’ field?

No. As this field routinely gets used for reporting purposes details of clients, staff members or other persons should not be identified in the ‘brief summary of the incident’ field of the incident report form. There are other fields in the incident report form appropriate for capturing these details.

## 9.14 How do I request an extension of due date for a CIMS investigation or review?

The CIMS IT functionality for requesting an extension of the due date for a CIMS investigation or review is essentially the same as when submitting an investigation or review outcome.

A request for an extension of the due date for a CIMS investigation or review is only applicable when the service provider is unable to continue an investigation or review due to circumstances outside the service provider’s control. An example of this would be if the incident involved a police investigation that cannot be conducted concurrently with a CIMS investigation.

Both users of the department-built client incident register and organisations using their own IT system / CIMS API apply for an extension of the due date electronically, via their CIMS IT.

**Requesting an investigation or review extension in the department-built client incident register**

To place an investigation on hold, go to the **Review outcomes** screen and follow these steps:

* Click in the **Outcome** field to select ‘Pending’ from the dropdown list. Further information is displayed, along with a link to a template.
* Select the **Incident investigation/review on hold request template** link. The template is available on the [CIMS webpage](http://providers.dhhs.vic.gov.au/cims) at <http://providers.dhhs.vic.gov.au/cims>.
* Complete the template and return to the **Investigation outcome** screen.
* Click **Update outcomes**.
* Attach the completed **Incident investigation/review on hold request template in the Upload documents attachments section.**
* **Submit and Confirm when completed and return to the Follow-up summary screen.**

Investigations or reviews that are put on hold will also have a revised due date created by the department’s divisional office.

The follow-up recommendation will be at a status of ‘Pending’.

For more information, see *Chapter 6 Major impact – follow up outcomes* of the CIMS [*Client incident register user manual*](https://providers.dhhs.vic.gov.au/sites/default/files/2020-02/Client%20incident%20register%20user%20manual%20-%20Client%20incident%20management%20system.docx)

## 9.15 What happens if I select ‘restricted access’ on an incident report?

When a service provider staff member selects ‘restricted access’ when submitting an incident report this will automatically result in:

* the incident report only being visible to the organisation’s chief executive officer or delegated authority (the chief executive officer or delegated authority can choose to remove this restriction)
* an escalation to a senior department delegate.

For most incidents, the service provider **should not** select to restrict access to the incident.

Where an incident is sensitive and where only the organisation’s chief executive officer or delegated authority has access to the incident report it is appropriate to restrict access to the incident.

## 9.16 What is the difference between the address details that I need to provide in the incident report?

* Address of Service Delivery:
  + Address of where the service was being provided to the client at the time of the incident.
  + Note: for residential services, enter the facility’s full street address rather than the facility’s name. For kinship or foster care, enter the full street address of the kinship or foster care placement. Addresses will be validated by Google.
* Area:
  + The DHHS area for where the service is delivered (see *Appendix A* of the CIMS [*Client incident report webform user manual*](https://providers.dhhs.vic.gov.au/sites/default/files/2018-12/Client%20incident%20report%20webform%20user%20manual_Client%20incident%20management%20system.docx)for list and map of DHHS service areas)
* Location of Incident:
  + The place where the incident occurred (eg: male bathroom at north end of Watsonia train station – platform 1)
* Address (within client section):
  + The client’s most recent, primary place of residence. If unknown, enter your organisation’s address. Address will be validated by Google.

## 9.17 When can I resubmit non-major impact incidents if they have been withdrawn by the department?

If a non-major impact incident report has been withdrawn by the department’s divisional office and needs to be resubmitted, the service provider should, review, revise and resubmit immediately (unless the incident report is out of scope for CIMS).

## 9.18 Do I need to save the incident report (department-built client incident register)?

Service providers completing an incident report in the department-built client incident register do not need to ‘save’ each incident report page. At the end of each page, the user just needs to click **Next** to move to the next section.

If the user needs to close the report and come back to it later to complete, the user can save it. They will be asked to provide an email address, and an email with a link and password will be sent to that address to allow the user to access the report at a later time. This function may be particularly useful if the service provider is concerned that the system will time-out while gathering information and completing the incident report.

The CIMS helpdesk (cims@dhhs.vic.gov.au) does not have access to see any saved incident reports and cannot advise what email address or password has been provided in the ‘save’ process.

It is not possible to view a partially completed (saved) report in the client incident register.

If a partially completed (saved) incident report cannot be retrieved by the user or service provider organisation, a new incident report must be created.

## 9.19 Can an organisation submit more documents for an outcome that has already been submitted?

Once an outcome (excluding ‘Pending’) has been received by the department, a service provider cannot submit additional information or attachments.

To allow an organisation to submit further information, the outcome must first be withdrawn by the department’s divisional office and then the outcome (including the new information) resubmitted.

Note: Further information including attachments can be submitted by an organisation without the requirement of the department withdrawing an outcome if the most recent outcome submission was ‘Pending’.

Once an outcome is endorsed, no additional documentation can be attached to the outcome.

## 9.20 How can I tell if my organisation is onboarded to CIMS IT?

A quick tip to check if your organisation has been onboarded (registered) to the CIMS:

* open the CIMS incident report webform on the CIMS webpage and start typing the name of your organisation in the ‘Organisation name’ field. If the organisation does not appear, then it is not onboarded to CIMS.

If in doubt, or you want to check the status of your organisation’s onboarding process, contact either the CIMS helpdesk via CIMS@dhhs.vic.gov.au or [cims.registration@dhhs.vic.gov.au](mailto:cims.registration@dhhs.vic.gov.au) for assistance.

## 9.21 Can an already approved incident report, follow-up recommendation or outcome be withdrawn?

Yes, the CIMS enables a ‘withdrawal admin’ user to withdraw incident reports, follow-up recommendations as required.

The process of withdrawing these items is exactly the same as a standard withdrawal with the service provider receiving a notification (which includes the reason and rationale) and the status reverting to withdrawn.

## 9.22 My organisation is not onboarded/registered yet to the CIMS application. How can we report an incident?

Service providers are required to ensure that they are registered to use the CIMS to submit and manage incident information.

If a service provider is not fully registered to use the CIMS application and needs to report a major impact incident as required under the CIMS policy, the service provider’s chief executive officer or senior delegate should contact the CIMS helpdesk via CIMS@dhhs.vic.gov.au. The CIMS helpdesk will arrange a one-off link that will enable the service provider to submit one major impact incident. After that, the service provider is required to complete the CIMS IT registration and onboarding process immediately.

## 9.23 An organisation is having trouble accessing its client incident register. Can they report outside of the system via the one-off direct submission link?

No. Since the implementation of CIMS, only electronic submissions for incident reports are accepted. The one-off link can only be provided to an organisation that is not onboarded to CIMS. Once the organisation has completed the process, the direct submission link is void. This includes organisations using either the department-built client incident register or their own/vendor system.

If an organisation is having problems with accessing the CIMS, they need to contact the CIMS helpdesk ([cims@dhhs.vic.gov.au](mailto:cims@dhhs.vic.gov.au)) for further assistance.

## 9.24 Who is responsible for updating service providers’ user details in the CIMS client incident register?

Service providers are responsible for updating (eg: adding, removing, editing) their staff user details in the CIMS. A CIMS Senior Delegate level user has the functionality to manage user provisioning. Please note however, that if a prospective user does not have an eBusiness account, they will need to contact the eBusiness Administrator on **1300 799 470** to arrange this first.

Step by step instructions on how to manage CIMS user access is in *Chapter 14 (Managing user profiles)* of the *CIMS IT Client Incident Register User Manual* available on the Department's CIMS web page: <https://providers.dhhs.vic.gov.au/client-incident-register-user-manual-cims-word> .

# Section 10 – Supports for service providers

## 10.1 Learning and development

Online learning (self-paced modules) and resource materials (user manuals and training environment to simulate completing an incident report) are available on the department’s CIMS webpage at <https://providers.dhhs.vic.gov.au/cims-learning-and-development>.

The department is not conducting any classroom-based training for CIMS at this point in time.

Please note that all learning and development materials are currently under review to incorporate the CIMS policy changes that were implemented on 3 February 2020.   Please familiarise yourself (if you haven’t done so already) with the CIMS policy changes that occurred by reading the *[CIMS policy update 1 - 2020](https://providers.dhhs.vic.gov.au/cims-policy-update-1-2020)*  release note and the [*Frequently Asked Questions – policy update 1 - 2020*](https://providers.dhhs.vic.gov.au/frequently-asked-questions-policy-update-1-2020)  document.

## 10.2 Helpdesk service

General queries regarding CIMS can be made to the CIMS helpdesk via [email](mailto:CIMS@dhhs.vic.gov.au) at [CIMS@dhhs.vic.gov.au](mailto:CIMS@dhhs.vic.gov.,au). The helpdesk is operational Monday to Friday (excluding public holidays) from 9.00am – 5.00 pm.

## 10.3 Toolkit

CIMS fact sheets, summary guide, templates, learning and development resources are available on the [CIMS page](http://providers.dhhs.vic.gov.au/cims) to support the application of the CIMS policy and processes.

|  |
| --- |
| To receive this publication in an accessible format phone 1300 650 172, using the National Relay Service 13 36 77 if required, or email [CIMS](mailto:CIMS@dhhs.vic.gov.au) <[CIMS.@dhhs.vic.gov.au](mailto:CIMS.@dhhs.vic.gov.au)>.  Authorised and published by the Victorian Government, 1 Treasury Place, Melbourne.  © State of Victoria, Australia, Department of Health and Human Services June 2020.  Available at the [CIMS page](https://providers.dhhs.vic.gov.au/cims) on the Service Providers website: <<https://providers.dhhs.vic.gov.au/cims>>. |